APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,154	11/03/2003	Massimiliano Antonio Poletto	12221-014001	5561

26161	7590	05/05/2006	

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
MEHRMANESH, ELMIRA

ART UNIT	PAPER NUMBER
2113	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03 November 2003</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-24</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-24</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>03 November 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

The application of Poletto et al., for a "Connection based anomaly detection" filed

November 3, 2003, has been examined.

Claims 1-24 are presented for examination.

Claim 24 rejected under 35 USC § 101.

Claims 1-5 and 8-23 are rejected under 35 USC § 102.

Claims 6 and 7 are rejected under 35 USC § 103.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 8-13, and 17-22 are provisionally rejected on the ground of nonstatutory

obviousness-type double patenting as being unpatentable over claims 5-10 of

copending Application No.10701356. Although the conflicting claims are not identical,

they are not patentably distinct from each other because of the following:

10701154	10701356
claims 8 and 17	claim 5
claims 9 and 18	claim 6
claims 10 and 19	claim 7
claims 11 and 20	claim 8
claims 12 and 21	claim 9
claims 13 and 22	claim 10

As per claims 8 and 17 of the instant application, claims 8 and 17 have the

common limitation of *"the connection table includes a plurality of records that are*

indexed by source address" with claim 5 of 10701356. This common limitation performs

the same function.

It would have been obvious to one of ordinary skill in the art at the time the

invention to use the indexing method of claims 8 and 17 of the instant application in the

connection table of claim 5 of 10701356.

One of ordinary skill in the art at the time the invention would have been

motivated to make the combination because according to the specifications of the

instant application using the source address to index records in a connection table will

be useful in detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871)

discloses the use of the source address to detect DoS attacks (page 5, paragraph

[0071] and page 6, paragraph [0081]).

As per claims 9 and 18 of the instant application, claims 9 and 18 have the

common limitation of *"the connection table includes a plurality of records that are

indexed by destination address"* with claim 6 of 10701356. This common limitation

performs the same function.

It would have been obvious to one of ordinary skill in the art at the time the

invention to use the indexing method of claims 9 and 18 of the instant application in the

connection table of claim 6 of 10701356.

One of ordinary skill in the art at the time the invention would have been

motivated to make the combination because according to the specifications of the

instant application using the source address to index records in a connection table will

be useful in detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871)

discloses the use of the data flow parameters to detect DoS attacks (page 5, paragraph

[0071] and page 6, paragraph [0081]).

As per claims 10 and 19 of the instant application, claims 10 and 19 have the

common limitation of *"the connection table includes a plurality of records that are

indexed by time"* with claim 7 of 10701356. This common limitation performs the same

function.

It would have been obvious to one of ordinary skill in the art at the time the invention to use the indexing method of claims 10 and 19 of the instant application in the connection table of claim 7 of 10701356.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because according to the specifications of the instant application using the time to index records in a connection table will be useful in detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871) discloses the use of the data flow parameters to detect DoS attacks (page 5, paragraph [0071] and page 6, paragraph [0081]).

As per claims 11 and 20 of the instant application, claims 11 and 20 have the common limitation of *"the connection table includes a plurality of records that are indexed by source address, destination address and time"* with claim 8 of 10701356. This common limitation performs the same function.

It would have been obvious to one of ordinary skill in the art at the time the invention to use the indexing method of claims 11 and 20 of the instant application in the connection table of claim 8 of 10701356.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because according to the specifications of the instant application using the source address, destination address and time to index records in a connection table will be useful in detecting the DoS attacks. Malan et al.

(U.S. PGPUB No. 20020032871) discloses the use of the data flow parameters to detect DoS attacks (page 5, paragraph [0071] and page 6, paragraph [0081]).

As per claims 12 and 21 of the instant application, claims 12 and 21 have the common limitation of *"the connection table includes a plurality of connection sub-tables to track data at different time scales"* with claim 9 of 10701356. This common limitation performs the same function.

It would have been obvious to one of ordinary skill in the art at the time the invention to use plurality of tables of claims 12 and 21 of the instant application in addition to the connection table of claim 9 of 10701356.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because according to the specifications of the instant application using plurality of tables in a connection table will be useful in detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871) discloses the use of multiple tables to categorize alert messages, which are used to detect DoS attacks and the source of attacks (page 5, paragraph [0074]).

As per claims 13 and 22 of the instant application, claims 13 and 22 have the common limitation of "the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of

records received from all collectors during respective units of time" with claim 10 of

10701356. This common limitation performs the same function.

It would have been obvious to one of ordinary skill in the art at the time the

invention to use plurality of tables of claims 13 and 22 of the instant application in

addition to the connection table of claim 10 of 10701356.

One of ordinary skill in the art at the time the invention would have been

motivated to make the combination because according to the specifications of the

instant application using plurality of tables in a connection table will be useful in

detecting the DoS attacks. Malan et al. (U.S. PGPUB No. 20020032871) discloses the

use of multiple tables to categorize alert messages, which are used to detect DoS

attacks and the source of attacks (page 5, paragraph [0074]).

This is a <u>provisional</u> obviousness-type double patenting rejection because the

conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

Claim 24 is rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

Claim 24 is a method *"method of detecting a failed host"* which results in an

abstract idea. The claim limitations are merely steps of a computation or a formula. The

limitations of "determining" and "indicating" describe a method where the result is an

abstract idea.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention.

The limitations "*greater than M*" and "*less than R*" are not definite and it is not

clear as to what the definitions of these limitations are according to the Specifications.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5 and 8-22 are rejected under 35 U.S.C. 102(e) as being anticipated by

Malan et al. (U.S. PGPUB No. 20020032871).

As per claim 1, Malan discloses a system, comprising:

a plurality of collector devices that are disposed to collect statistical information

on packets that are sent between nodes on a network (page 5, paragraph [0066]) and

(Fig. 4, elements 20, 20b).

an aggregator (page 5, paragraph [0071], lines 7-11) and (page 3, paragraphs

[0032], [0033], and [0034]) that receives network data from the plurality of collector

devices, and which produces a connection table that maps each node on the network to

a record that stores information about traffic to or from the node (page 5, paragraphs

[0066] and [0067]).

As per claim 2, Malan discloses the aggregator determines occurrences of

network events (page 5, paragraph [0071] and page 3, paragraph [0032]).

As per claim 3, Malan discloses the aggregator further comprises: a process that

communicates occurrences of network events to an operator (page 6, paragraph [0075],

lines 8-13 and page 7, paragraph [0086], lines 1-10).

As per claim 4, Malan discloses the aggregator device further comprises: a

process to aggregate anomalies into the network events (page 5, paragraph [0071] and

page 3, paragraph [0032]).

As per claim 5, Malan discloses the collectors have a passive link to devices in the network (FIG. 7).

As per claim 8, Malan discloses the connection table includes a plurality of records that are indexed by source address (page 5, paragraph [0067], lines 10-14).

As per claim 9, Malan discloses the connection table includes a plurality of records that are indexed by destination address (page 5, paragraph [0067], lines 10-14).

As per claim 10, Malan discloses the connection table includes a plurality of records that are indexed by time (page 5, paragraph [0067], lines 10-14).

As per claim 11, Malan discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (page 5, paragraph [0067], lines 10-14).

As per claim 12, Malan discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (page 5, paragraph [0074]).

As per claim 13, Malan discloses the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table

holding the sum of records received from all collectors during respective units of time

(page 5, paragraph [0074]).

As per claim 14, Malan discloses a method, comprises:

providing a plurality of collector devices in a network to collect statistical

information on packets that are sent between nodes on a network (page 5, paragraph

[0066]) and (Fig. 4, elements 20, 20b) and sending statistical information from the

collector devices to an aggregator (page 5, paragraph [0071], lines 7-11) and (page 3,

paragraphs [0032], [0033], and [0034]), the aggregator producing a connection table

that maps each node on the network to a record that stores information about traffic to

or from the node (page 5, paragraphs [0066] and [0067]).

As per claim 15, Malan discloses the aggregator determines occurrences of

network events (page 5, paragraph [0071] and page 3, paragraph [0032]).

As per claim 16, Malan discloses aggregating anomalies into the network events

and communicating occurrences of network events to an operator (page 6, paragraph

[0075], lines 8-13).

As per claim 17, Malan discloses the connection table includes a plurality of

entries that are indexed by source address (page 5, paragraph [0067], lines 10-14).

As per claim 18, Malan discloses the connection table includes a plurality of entries that are indexed by destination address (page 5, paragraph [0067], lines 10-14).

As per claim 19, Malan discloses the connection table includes a plurality of records that are indexed by time (page 5, paragraph [0067], lines 10-14).

As per claim 20, Malan discloses the connection table includes a plurality of records that are indexed by source address, destination address and time (page 5, paragraph [0067], lines 10-14).

As per claim 21, Malan discloses the connection table includes a plurality of connection sub-tables to track data at different time scales (page 5, paragraph [0074]).

As per claim 22, Malan discloses the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table with each sub-table holding the sum of records received from all collectors during respective units of time (page 5, paragraph [0074]).

Claim 23 is rejected under 35 U.S.C. 102(e) as being anticipated by Belissent (U.S. Patent No. 6,789,203).

As per claim 23, Malan discloses a method of detecting a new host connecting to a network comprises:

receiving statistics collected from a host in the network (page 5, paragraphs [0066] and [0067]).

Malan fails to explicitly disclose the relation of received packets over a period of time.

Belissent teaches:

and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T (col. 4, lines 9-20 and col. 5, lines 62-67 through col. 6, lines 1-17). Belissent discloses a system for monitoring connection request rates over a period of time and a rejection threshold.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Malan et al. (U.S. PGPUB No. 20020032871) in view of Hill et al. (U.S. Patent No. 6,088,804).

As per claim 6, Malan discloses the anomalies include denial of service attacks (page 4, paragraph [0057]).

Malan et al. fails to explicitly disclose scanning attacks.

Hill teaches:

the anomalies include and scanning attacks (col. 4, lines 35-41).

As per claim 7, Malan et al. fails to explicitly unauthorized access and worm propagation.

Hill teaches:

the anomalies include unauthorized access and worm propagation (col. 5, lines 57-65).

It would have been obvious to one of ordinary skill in the art at the time the invention to use the network security attack detection system of Hill et al.'s in combination with the network anomaly detection system of Malan et al. to effectively detect network anomalies.

One of ordinary skill in the art at the time the invention would have been motivated to make the combination because both inventions disclose a method of blocking security attacks in a network. Malan et al. discloses a system to detect and block DoS attacks by collecting network data statistics (page 3, paragraph [0028] and [0029]). Hill et al. discloses a method and system to respond to security attacks by collecting data through security agents (col. 3, lines 17-30 and col. 4, lines 53-61).

Related Prior Art

The following prior art is considered to be pertinent to applicant's invention, but nor relied upon for claim analysis conducted above.

Gleichauf et al. (U.S. Patent No. 6,499,107), "Method and system for adaptive network security using intelligent packet analysis".

Lin et al. (U.S. Patent No. 6,751,668), "Denial-of-service attack blocking with selective passing and flexible monitoring".

Belissent (U.S. Patent No. 6,789,203), "Method and apparatus for preventing a denial of service (DOS) attack by selectively throttling TCP/IP requests".

Bartucca et al. (U.S. Patent No. 6,918,067), "Detecting network instability".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Elmira Mehrmanesh whose telephone number is (571) 272-5531. The examiner can normally be reached on 8-5 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Robert W. Beausoliel can be reached on (571) 272-3645. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

ROBERT BEAUSOLIEL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100